THE TAXBOOK News Release Date: 10/4/22

IRS Warns Taxpayers of Texting Scams

Cross References

- IR-2022-167, September 28, 2022

The Internal Revenue Service is warning taxpayers of a recent increase in IRS-themed texting scams aimed at stealing personal and financial information.

So far in 2022, the IRS has identified and reported thousands of fraudulent domains tied to multiple MMS/SMS/text scams (known as smishing) targeting taxpayers. In recent months, and especially in the last few weeks, IRS-themed smishing has increased exponentially.

Smishing campaigns target mobile phone users, and the scam messages often look like they're coming from the IRS, offering lures like fake COVID relief, tax credits or help setting up an IRS online account. Recipients of these IRS-related scams can report them to phishing@irs.gov.

"This is phishing on an industrial scale so thousands of people can be at risk of receiving these scam messages," said IRS Commissioner Chuck Rettig. "In recent months, the IRS has reported multiple large-scale smishing campaigns that have delivered thousands—and even hundreds of thousands—of IRS-themed messages in hours or a few days, far exceeding previous levels of activity."

With the approach of October's Cybersecurity Awareness Month, the IRS and the Security Summit partners in the states and the nation's tax community remind people and the tax professional community to be on the lookout for phishing scams and other schemes that could put sensitive tax data at risk.

In the latest activity, the scam texts often ask taxpayers to click a link where phishing websites will try to collect their information or potentially send malicious code onto their phones. The IRS does not send emails or text messages asking for personal or financial information or account numbers. These messages should all be red flags for taxpayers.

Beginning in the fall of 2020, the IRS observed an increase in reports of smishing scams requesting taxpayer personal and financial information. These smishing campaigns continued through the pandemic. The IRS has taken numerous steps to warn people of this ongoing threat, including posting a video about how to avoid IRS text message scams.

Taxpayers should continue reporting these scams to phishing@irs.gov. Their reporting allows the IRS to report these scams to the appropriate service providers for action, protecting other taxpayers who might receive a variant of the same scam.

While the IRS works to shut down online fraud, criminals are using ever-evolving tactics to cast a wider net and catch more victims, like using algorithms to automatically generate hundreds or even thousands of fraudulent domains. For example, a recent campaign used just three dozen stolen or bogus email addresses to create over 1,000 fraudulent domains.

"Particularly in these cases, the best offense is a good defense," said Rettig. "Taxpayers and tax pros need to remain constantly vigilant with suspicious IRS-related emails and text messages. And if you get one, sending the IRS important details from the text can help us disrupt the scams and protect others."

Reporting IRS-related smishing. The IRS maintains an inbox, phishing@irs.gov, to process IRS, Treasury and/or tax-related online scams only. Smishing involving other agencies and/or brands should not be reported to phishing@irs.gov.

Reporting IRS-themed texts to the IRS allows security professionals to track and disrupt these scams. Individuals reporting scam texts to the IRS should include both the body of the message and the sender's information in one email or text. Copying the actual text into an email is preferred. However, if necessary, screenshots can be sent. Scam SMS/text messages can also be copied and forwarded to wireless providers via text to 7726 (SPAM), which helps them spot and block similar messages in the future.

The following process will help capture important details for reporting smishing to the IRS:

- Create a new email to phishing@irs.gov.
- Copy the caller ID number (or email address).
- Paste the number (or email address) into the email.
- Press and hold the SMS/text message and select "copy".
- Paste the message into the email.
- If possible, include the exact date, time, time zone and telephone number that received the message.
- Send the email to phishing@irs.gov.

Additional reporting. In addition to reporting the scam to phishing@irs.gov, if IRS-related, report the message to the Treasury Inspector General for Tax Administration using their IRS Impersonation Scam Reporting form and the Federal Trade Commission (FTC) through their Complaint Assistant to make the information available to investigators.

All incidents, successful and attempted, should also be reported to the Internet Crime Complaint Center.

Any individual entering personal information, or otherwise finding themselves a victim of tax-related scams, can find additional resources at Identity Theft Central on IRS.gov.